Boolean Functions, Projection Operators and Quantum Error Correcting Codes

Vaneet Aggarwal and Robert Calderbank
Department of Electrical Engineering, Princeton University, NJ 08544, USA
Email: {vaggarwa, calderbk}@princeton.edu

***Abstract*—This paper describes a fundamental correspondence between Boolean functions and projection operators in Hilbert space. The correspondence is widely applicable, and it is used in this paper to provide a common mathematical framework for the design of both additive and non-additive quantum error correcting codes. The new framework leads to the construction of a variety of codes including an infinite class of codes that extend the original $((5, 6, 2))$ code found by Rains [21]. It also extends to operator quantum error correcting codes.**

***Index Terms*—Quantum Error Correction, projection operators in Hilbert space, Boolean functions, additive and non-additive quantum codes, operator quantum error correction.**

I. Introduction

The additive or stabilizer construction of *quantum error correcting codes* (QECC) takes a classical binary code that is self-orthogonal with respect to a certain symplectic inner product, and produces a quantum code, with minimum distance determined by the classical code (for more details see [7], [8] and [14]). The first non-additive quantum error-correcting code was constructed by Rains *et al.* [21]. This code was constructed numerically by building a projection operator with a given weight distribution. Grassl and Beth [13] generalized this construction by introducing union quantum codes, where the codes are formed by taking the sum of subspaces generated by two quantum codes. Roychowdhury and Vatan [23] gave some sufficient conditions for the existence of nonadditive codes, and Arvind *et al.* [5] developed a theory of non-additive codes based on the Weyl commutation relations. Most recently, Kribs *et al.* [16] introduced *operator quantum error correction* (OQEC) which unifies the standard error correction model, the method of decoherence-free subspaces, and that of noiseless subsystems.

We will describe, what we believe to be the first mathematical framework for code design that encompasses both additive and non-additive quantum error correcting codes. It is based on a correspondence between Boolean functions and projection operators in Hilbert space that is described in Sections II and III. We have used an initial version of this correspondence to construct Grassmannian packings [1] and space-time codes for wireless communication [3]. However, the correspondence in Section III applies to a larger class of projection operators and includes the correspondence described in [3] as a special case (see Section IV). We note that prior work by Danielson [11] interpreted Boolean functions as quantum states and developed a correspondence between Boolean functions and zero-dimensional quantum codes.

After introducing the fundamentals of quantum error correcting codes in Section V, we will derive in Section VI sufficient conditions for existence of QECC in terms of existence of certain Boolean function. This paper goes beyond deriving sufficient conditions, and constructs the quantum code if these properties are satisfied. Hence, we convert the problem of finding a quantum code into a problem of finding Boolean function satisfying certain properties. We also see how certain well-known codes fit into this scheme. We focus on non-degenerate codes which is defensible given that we know of no parameters k, M and d for which there exists a $((k, M, d))$ degenerate QECC but not a $((k, M, d))$ non-degenerate QECC (see [2]). Further, in Section VII, we describe how this scheme fits into a general framework of operator quantum error correcting codes. More precisely, we give sufficient conditions for the existence of $((k, M, N, d))$ stabilizer OQEC and also construct the code if these conditions are satisfied.

II. Boolean Function

A *Boolean function* is defined as a mapping $f : \{0, 1\}^m \rightarrow \{0, 1\}$[20]. The mapping $v = \sum_{i=1}^{m} v_i 2^{i-1}$ associates an integer v from the set $\{0, 1, ..., 2^m - 1\}$ with a binary m-tuple $(v_m, ..., v_1)$ with $v_i \in \{0, 1\}$. (Throughout the paper, $\sum$ represents addition over integers.) This integer is called the *decimal index* for a given m-tuple.

An m-variable Boolean function f can be specified by listing the values at all decimal indices. The binary-valued vector of function values $Y = [y_0, y_1, ..., y_{2^m-1}]$ is called the *truth vector* for f.

An m-variable Boolean function $f(v_1, ..., v_m)$ can be represented as $\sum_{i=0}^{2^m-1} y_i v_1^{c_0(i)} v_2^{c_1(i)} ....v_m^{c_{m-1}(i)}$ where y_j is the value of the Boolean function at the decimal index j and $c_0(j)$, $c_1(j)$, ... , $c_{m-1}(j) \in \{0, 1\}$ are the coordinates in the binary representation for j (with c_{m-1} as the most significant bit and c_0 as the least significant bit) with $v_j^1 = v_j$ and $v_j^0 = \bar{v}_j$ (Theorem 7.7, [18]).

Example 1: The truth vector of the three-variable Boolean function $f(v_1, v_2, v_3) = v_1 v_2 \bar{v_3}$ is $Y = [0, 0, 0, 1, 0, 0, 0, 0]$

This work was supported in part by AFOSR under contract 00852833. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Nice, France, June 2007.

Definition 1: The *Hamming weight* of a Boolean function is defined as the number of nonzero elements in Y.

Definition 2 ([20]): Let $\oplus$ denote modulo two addition. The *(periodic) autocorrelation function* of a Boolean function $f(v)$ at a is the inner product of f with a shift of f by a. More precisely, $r(a) = \sum_{v=0}^{2^m-1} (-1)^{f(v)\oplus f(v\oplus a)}$ where $a \in \{0, 1, ..., 2^m - 1\}$, $a = \sum_{i=1}^{m} a_i 2^{i-1}$. An autocorrelation function is represented as a vector $R = [r(0), r(1), ...r(2^m - 1)]$

Definition 3: The *complementary set* of a Boolean function $f(v)$ is defined by $Cset_f = \{a| \sum_{v=0}^{2^m-1} f(v)f(v \oplus a) = 0\}$

This means that for any element a in the $Cset_f$, $f(v)f(v \oplus a) = 0$ for any choice of $v \in \{0, 1, ..., 2^m - 1\}$. The complementary set links distinguishability in the quantum world (orthogonality of subspaces) with properties of Boolean functions. The quantity $f(v \oplus a)$ is the counterpart in the quantum world of the quantum subspace after the error has occurred, which is to be orthogonal to the original subspace corresponding to $f(v)$ as will be described in later sections.

Lemma 1: If the Hamming weight of the Boolean function f is M, and $M \leq 2^{m-1}$, then the complementary set $Cset_f = \{a|r(a) = 2^m - 4M\}$

Proof: If $a \in Cset_f$ then $f(v)f(v \oplus a) = 0$ for all $v = 0, 1, ..., 2^m - 1$ and the supports of f(v) and $f(v \oplus a)$ are disjoint. Hence

$$\begin{aligned} r(a) &= \sum_{v=0}^{2^m-1} (-1)^{f(v)\oplus f(v\oplus a)} \\ &= (-1)^1 M + (-1)^1 M + (-1)^0 (2^m - 2M) \\ &= 2^m - 4M \end{aligned}$$

Conversely suppose

$$r(a) = \sum_{v=0}^{2^m-1} (-1)^{f(v)\oplus f(v\oplus a)} = 2^m - 4M.$$

If the supports of $f(v)$, $f(v\oplus a)$ intersect in N decimal indices then

$$\begin{aligned} r(a) &= N - 2(M - N) + (2^m - 2(M - N) - N) \\ &= 2^m - 4M + 4N \end{aligned}$$

Hence, $N = 0$ and $a \in Cset_f$. ■

Example 2: Let $f(v_1, v_2, v_3) = v_1 v_2 \bar{v_3}$. Then the vector B corresponding to the autocorrelation function is $[8, 4, 4, 4, 4, 4, 4, 4]$, and $Cset_f = \{1, 2, 3, 4, 5, 6, 7\}$.

III. Boolean Functions and a Logic of Projection Operators

The authors of [3] connected Boolean logic to projection operators derived from the Heisenberg-Weyl group. In this section, we generalize these results to a larger class of projection operators.

Let $\mathbb{B}(H)$ be the set of bounded linear operators on a Hilbert space H. An operator $P \in \mathbb{B}(H)$ is called a projection operator (sometimes we will use the terms orthogonal projection operator and self-adjoint projection operator) on H iff $P = PP^\dagger$. We denote the set of projection operators on H by $\mathbb{P}(H)$ and the set of all subspaces of H by $\mathbb{L}(H)$.

Definition 4:
1) If $S \subseteq H$, the span of S is defined as $\vee S = \cap\{K|K$ is a subspace in H with $S \subseteq K\}$. It is easy to see that $\vee S$ is the smallest subspace in H containing S.
2) If $S \subseteq H$, the orthogonal complement of S is defined as $S^\perp = \{x \in H|x \perp s$ for all $s \in S\}$.
3) If $\mathbb{S}$ is a collection of subsets of H, we write $\vee_{S\in\mathbb{S}} S = \vee(\cup_{S\in\mathbb{S}} S)$.

Definition 5: Let $P \in \mathbb{P}(H)$ and let $K = image(P) = \{Px|x \in H\}$. We call P the projection of H onto K. Two projections P and Q onto K and L are orthogonal (denoted $P \perp Q$) if $PQ = 0$. It is easy to verify that $PQ = 0 \Leftrightarrow K \perp L \Leftrightarrow QP = 0$. (Theorem 5B.9, [10])

Definition 6: Let $P, Q \in \mathbb{P}(H)$ with $K = image(P)$ and $L = image(Q)$. Then

- $P < Q$ iff K$\subset$ L ($K \neq L$)
- $P \vee Q$ is the projection of H onto $K \vee L$
- $P \wedge Q$ is the projection of H onto $K \cap L$.
- $\tilde{P}$ is the projection of H onto $K^\perp$.

The structure $(\mathbb{P}(H), \leqslant, \perp)$ is a logic with unit I_H (identity map on H) and zero Z_H (zero map on H) (Theorem 5B.18, [10]). This logic is called *Projection Logic*.

Lemma 2 (Theorem 5B.18, [10]): The map $P \rightarrow image(P)$ from $\mathbb{P}(H)$ to $\mathbb{L}(H)$ is a bijection that preserves order, orthogonality, meet($\wedge$) and join($\vee$).

Lemma 3 ([10]): If $<< P_k >>$ are pairwise orthogonal projection operators, in $\mathbb{P}(H)$, then $\vee_{k=1}^{\infty} P_k = \sum_{k=1}^{\infty} P_k$.

Lemma 4 ([10]): If $P, Q \in \mathbb{P}(H)$, then

1) $PQ = QP$ iff PQ is a projection.
2) If PQ is a projection, $image(PQ) = image(P) \cap image(Q)$.

Lemma 5: If P and Q are commutative operators, then the distributive law holds (and this law fails to hold for non-commutative operators). Also, in this case,

1) $P \wedge Q = PQ$
2) $P \oplus Q \triangleq (P \wedge \tilde{Q}) \vee (\tilde{P} \wedge Q) = P + Q - 2PQ$
3) $\tilde{P} = I - P$
4) $P \vee Q = P + Q - PQ$

Proof:

1) From Lemma 4, $image(PQ) = image(P) \cap image(Q)$. Hence, $image(PQ) = image(P \wedge Q)$ and by Lemma 2, $P \wedge Q = PQ$.

2) We have

$$\begin{aligned} P+Q-2PQ &= P(I-Q)+Q(I-P) \\ &\overset{(a)}{=}[P(I-Q)]\vee[Q(I-P)] \\ &\overset{(b)}{=}[P\wedge(I-Q)]\vee[Q\wedge(I-P)] \\ &\overset{(c)}{=}P\oplus Q. \end{aligned}$$

where (a) follows from Lemma 3, (b) follows from Lemma 4 and (c) follows directly from definition of $P\oplus Q$.

3) $\tilde{P}=I-P$ follows directly from Definition 6.

4) We have

$$\begin{aligned} (P\oplus Q)\vee(P\wedge Q) &\overset{(d)}{=}(P\oplus Q)+(P\wedge Q) \\ &\overset{(e)}{=}P+Q-2PQ+PQ \\ &=P+Q-PQ \end{aligned}$$

Also, $(P\oplus Q)\vee(P\wedge Q)$

$$\begin{aligned} &=(P\wedge\tilde{Q})\vee(\tilde{P}\wedge Q)\vee(P\wedge Q) \\ &\overset{(f)}{=}(P\wedge\tilde{Q})\vee((\tilde{P}\vee P)\wedge Q) \\ &=(P\wedge\tilde{Q})\vee Q \\ &\overset{(g)}{=}(P\vee Q)\wedge(\tilde{Q}\vee Q) \\ &=(P\vee Q) \end{aligned}$$

where (d) follows from Lemma 3 since $P\oplus Q$ and $P\wedge Q$ are orthogonal ($(P+Q-2PQ)PQ=0$), (e) follows from Lemma 4, and (f), (g) follows from the distributive laws. Hence, $P\vee Q=P+Q-PQ$. ■

Next we define projection functions following [3].

Definition 7: Given an arbitrary Boolean function $f(v_1,....,v_m)$, we define the *projection function* $f(P_1,...,P_m)$ in which v_i in the Boolean function is replaced by P_i, multiplication in the Boolean logic is replaced by the meet operation in the projection logic, summation in the Boolean logic (or the *or* function) is replaced by the join operation in the projection logic and the not operation in Boolean logic is replaced by the tilde ($\tilde{P}$) operation in the projection logic.

As is standard when writing Boolean functions, we use *xor* (modulo 2 addition, represented by $\oplus$) in place of *or*, hence by above definition, we will replace the *xor* in the Boolean logic by the *xor* operation in the projection logic.

Theorem 1: If $(P_1,...,P_m)$ are pairwise commutative projection operators of dimension 2^{m-1} such that $P_1P_2..P_m$, $P_1P_2..\tilde{P}_m$, ... $\tilde{P}_1\tilde{P}_2..\tilde{P}_m$ are all one-dimensional projection operators and H is of dimension 2^m, then $P_f=f(P_1,....P_m)$ is an orthogonal projection on a subspace of dimension $Tr(P_f)=wt(f)$, where $wt(f)$ is the Hamming weight of the Boolean function f.

Proof: By definition of $f(P_1,....P_m)$, we have a representation of P_f in terms of meet, join and tilde operations in the corresponding projection logic. By Lemma 2, every function of projection operators in terms of meet, join and tilde will be present in the projection logic. Hence, P_f is an orthogonal projection operator and this proves the first part of the theorem. Now, we will find the dimension of this projection operator. $f(v_1,v_2,..,v_m)$ can be represented as $\sum_{i=0}^{2^m-1} y_i v_1^{c_0}v_2^{c_1}....v_m^{c_{m-1}}$ as described in Section II. If $wt(f)=M$, then M terms of y_i are 1 and the remaining terms are 0. Also, in this case, $P_f=f(P_1,P_2,..,P_m)=\bigvee_{i=0}^{2^m-1} y_iP_1^{c_0}P_2^{c_1}....P_m^{c_{m-1}}$ (where $P_j^1=P_j$ and $P_j^0=\tilde{P}_j$). Hence, the image of P_f is the minimum subspace containing all $y_iP_1^{c_0}P_2^{c_1}....P_m^{c_{m-1}}$. We know by the statement of the theorem that the dimension of $P_1^{c_0}P_2^{c_1}....P_m^{c_{m-1}}$ is 1 for all $c_0,c_1,...,c_{m-1}\in\{0,1\}$, and all these subspaces are orthogonal. Also, the minimum subspace containing all these operators is the whole Hilbert space. So, the dimension of P_f will be the sum of dimensions of $y_iP_1^{c_0}P_2^{c_1}....P_m^{c_{m-1}}$ for all i (which is 1 when y_i = 1, and 0 otherwise). Hence, the dimension of P_f is M. ■

Theorem 1 is a generalization of the Theorem 1 of [3] because we consider *any* pairwise commutative projection operators, while in [3], a special case of commutative projection operators using Heisenberg-Weyl group was used. This special case is described in Section IV. Hence, to prove Theorem 1, we use abstract properties of projection logic [10] rather than the properties of a particular commutative subgroup.

Example 3: The Boolean function $f(v)=v_1\bar{v}_2+v_2\bar{v}_3$ corresponds to the operator $P_f=f(P_1,P_2,P_3)=(P_1\wedge\tilde{P}_2)\oplus(P_2\wedge\tilde{P}_3)$. If P_1,P_2,P_3 are pairwise commutative, then $P_f=P_1+P_2-P_1P_2-P_2P_3$.

IV. The Construction of Commutative Projection Operators from the Heisenberg-Weyl Group

Let X, Y, and Z be the Pauli matrices, given by

$$X=\begin{bmatrix}0&1\\1&0\end{bmatrix}, Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}, Y=\begin{bmatrix}0&i\\-i&0\end{bmatrix},$$

and consider linear operators E of the form $E=e_1\otimes\ldots\otimes e_m$, where $e_j\in\{I_2,X,Y,Z\}$. We form the *Heisenberg-Weyl group* (sometimes in the literature this group is referred to as an extraspecial 2-group or as the Pauli group) E_m of order 4^{m+1}, which is realized as the group of linear operators $\alpha E,\alpha=\pm1,\pm i$. (For a detailed description of the Heisenberg-Weyl group and its use to construct quantum codes see [7], [8].)

Next we define the symplectic product of two vectors and the symplectic weight of a vector.

Definition 8: The *symplectic inner product* of vectors $(a,b),(a',b')\in\mathbb{F}_q^{2m}$ is given by

$$(a,b)\odot(a',b')=a\cdot b'\oplus a'\cdot b. \tag{1}$$

Definition 9: The *symplectic weight* of a vector (a,b) is the number of indices i at which either a_i or b_i is nonzero.

The center of the group E_m is $\{\pm I_{2^m}, \pm iI_{2^m}\}$ and the quotient group $\overline{E}_m$ is isomorphic to the binary vector space $\mathbb{F}_2^{2m}$. We associate with binary vectors $(a,b) \in \mathbb{F}_2^{2m}$ operators $E_{(a,b)}$ defined by

$$E_{(a,b)} = e_1 \otimes \ldots \otimes e_m, \tag{2}$$

$$\text{where } e_i = \begin{cases} I_2, & a_i = 0, b_i = 0, \\ X, & a_i = 1, b_i = 0, \\ Z, & a_i = 0, b_i = 1, \\ Y, & a_i = 1, b_i = 1. \end{cases}$$

Lemma 6:

$$E_{(a,b)}E_{(a',b')} = (-1)^{b\cdot a'} i^{a\cdot b' + a'\cdot b} E_{(a\oplus a', b\oplus b')}.$$

Lemma 7:

$$E_{(a,b)}E_{(a',b')} = (-1)^{(a,b)\odot(a',b')} E_{(a',b')}E_{(a,b)}.$$

Thus $E_{(a,b)}$ and $E_{(a',b')}$ commute iff (a,b) and (a',b') are orthogonal with respect to the symplectic inner product (1).

We will now describe how to construct commutative projection operators. Take m linearly independent vectors $y_1, y_2, ..., y_m$ of length $2m$ bits with the property that the symplectic product between any pair is equal to zero. If we take $P_i = \frac{1}{2}(I + E_{y_i})$, then P_1, ... P_m satisfy all the properties of Theorem 1 and hence, $f(P_1, ...P_m)$ is an orthogonal projection operator [3].

Example 4: Take $f(v) = f(v_3, v_2, v_1) = v_1 + v_1v_2 + v_3$. Take y_1, y_2 and y_3 as $(1,0,0,0,1,0)$, $(0,1,1,1,1,0)$ and $(0,0,1,0,1,1)$ respectively which are linearly independent with all pairwise symplectic products equal to zero. Then $P_f = P_1 \oplus P_1P_2 \oplus P_3 = P_1 + P_3 - 2P_1P_3 - P_1P_2 + 2P_1P_2P_3$ where $P_i = \frac{1}{2}(I + E_{y_i})$, that is

$$P_f = \frac{1}{4}\begin{pmatrix} 2 & i & -1 & 0 & 0 & -i & 1 & 0 \\ -i & 2 & 0 & 1 & i & 0 & 0 & -1 \\ -1 & 0 & 2 & -i & -1 & 0 & 0 & -i \\ 0 & 1 & i & 2 & 0 & 1 & i & 0 \\ 0 & -i & -1 & 0 & 2 & i & 1 & 0 \\ i & 0 & 0 & 1 & -i & 2 & 0 & -1 \\ 1 & 0 & 0 & -i & 1 & 0 & 2 & -i \\ 0 & -1 & i & 0 & 0 & -1 & i & 2 \end{pmatrix}$$

V. Fundamentals of Quantum Error Correction

A $((k,M))$ quantum error correcting code is an M-dimensional subspace of $\mathbb{C}^{2^k}$. The parameter k is the code-length and the parameter M is the dimension or the size of the code. Let Q be the quantum code, and P be the corresponding orthogonal projection operator on Q. (For a detailed description, see [4].)

Definition 10: An error operator E is called *detectable* iff $PEP = c_E P$, where c_E is a constant that depends only on E.

Following [12], we restrict attention to the errors in the Heisenberg-Weyl group. Next, we define the minimum distance of the code.

Definition 11: The *minimum distance* of Q is the maximum integer d such that any error E, with symplectic weight at most $d-1$, is detectable.

The parameters of the quantum error correcting code are written $((k,M,d))$ where the third parameter d is the minimum distance of Q. We say that a $((k,M,d))$ quantum error correcting code exists if there exists a $((k,M))$ quantum error correcting code with minimum distance $\geq d$. We assume $d \geq 2$ throughout the paper. We also focus on non-degenerate $((k,M,d))$ codes, for which $PEP = 0$ for all errors E of symplectic weight $\leq d-1$, which is a sufficient condition for existence of the quantum code.

For any quantum code Q, we define the *stabilizer* H_Q as

$$H_Q = \{E \in E_k : E|x> = |x> \text{ for all } |x> \in Q\}$$

where E_k is the Heisenberg-Weyl group defined in Section IV. Then H_Q is an abelian group and is isomorphic to GF$(2)^m$, for some m. A quantum code is called *additive* or a *stabilizer* code if it is defined by its stabilizer H_Q, i.e.

$$Q = \{|x> \in \mathbb{C}^{2^k} : E|x> = |x> \text{ for all } E \in H_Q\}$$

A quantum code is non-additive if it is not equivalent to an additive code [22].

VI. Quantum Error Correcting codes with minimum distance d

We use $*$ to denote the standard binary inner product.

Theorem 2: A Boolean function f with the following properties determines a $((k,M,d))$-QECC

1) f is a function of k variables and has weight M.
2) There are $2k$ binary k-tuples $x_1, x_2, ..., x_{2k}$ such that $Cset_f$ contains the set $\{[x_1, x_2, ...x_{2k}] * w^T |$ w is a 2k bit vector of symplectic weight $\leq d-1\}$. The rows of the matrix A_f = $[x_1x_2.....x_{2k}]_{k\times 2k}$ have pairwise symplectic product zero and are linearly independent.

The projection operator corresponding to the QECC is obtained as follows:

(i) Construct the matrix A_f as above.
(ii) Define k projection operators each of the form $\frac{1}{2}(I+E_y)$ where y is a row of the matrix A_f, with P_k corresponding to the 1^{st} row, P_{k-1} corresponding to the 2^{nd} row and so on, so that P_1 corresponds to the last row.
(iii) Transform the Boolean function f into the projection operator P_f using Definition 7 where the commutative projection operators P_1 .... P_k are determined by the matrix A_f.

Proof: Consider a Boolean function $f(v)$ satisfying conditions 1) and 2). It follows easily from Section III and IV that P_f constructed as above is an M-dimensional projection operator. It remains to prove that the minimum distance is at

least d, so we need to show that $P_f\eta P_f\eta = 0$ for any error η in E_k with symplectic weight at most $d-1$.

An error η in E_k transforms the projection operator P_f to $P'_f = \eta P_f \eta$, and the condition $P_f\eta P_f\eta = 0$ means that P'_f is orthogonal to P_f. Denote by η_i the error represented by the binary $2k$-tuple with entry 1 in position i and zeros elsewhere. We emphasize that the subscripts i in x_i, η_i and $A_{j,i}$ ($(j,i)^{th}$ entry in the matrix A_f) are read modulo $2k$, so that x_{2k+1} is just x_1.

If $A_{1,k+1} = 0$ then η_1 commutes with P_k and $\eta_1 P_k \eta_1 = P_k$, and if $A_{1,k+1} = 1$ then $\eta_1 P_k \eta_1 = \tilde{P}_k$. In general, if $A_{k+1-j,k+i} = 0$ then $\eta_i P_j \eta_i = P_j$, and if $A_{k+1-j,k+i} = 1$ then $\eta_i P_j \eta_i = \tilde{P}_j$. Let $\eta_i P_j \eta_i = Q_{i,j}$ where $Q_{i,j} = P_j$ or $\tilde{P}_j$ and observe that $Q_{i,j} = P_j$ if and only if entry $(k+1-j)$ of x_{k+i} is zero. Then $\eta_i P_f \eta_i = f(Q_{i,1}, Q_{i,2}, ..., Q_{i,k})$ and the entries of x_{k+i} determine $\eta_i P_f \eta_i$. In fact, this correspondence can easily be understood in terms of the fundamental correspondence between between Boolean functions and projection operators, since the operator $\eta_i P_f \eta_i$ corresponds to the Boolean function $f(v \oplus x_{k+i})$.

When $d = 2$, we need to take care of all errors of symplectic weight 1 by showing $P_f\eta_i P_f \eta_i = 0$ and $P_f \eta_i \eta_{i+k} P_f \eta_i \eta_{i+k} = 0$. Applying the fundamental correspondence between Boolean functions and projection operators, this is equivalent to showing $f(v)f(v \oplus x_{k+i}) = 0$ and $f(v)f(v \oplus x_{k+i} \oplus x_i) = 0$ for all decimal indices v. This follows from the assumption that x_{k+i} and $x_{k+i} \oplus x_i$ are in the complementary set $Cset_f$..

In general we need to show that $P_f\eta P_f\eta = 0$ for all errors η of symplectic weight at most $d-1$. We write $\eta = \prod_{i \in A} \eta_i$, apply the fundamental correspondence, and find that $P_f\eta P_f\eta$ corresponds to the Boolean function $f(v \oplus (\underset{i\in A}{\oplus} x_{i+k}))$. By assumption, $\underset{i\in A}{\oplus} x_{i+k}$ is in the complementary set $Cset_f$, so $f(v)f(v \oplus (\underset{i\in A}{\oplus} x_{i+k})) = 0$ for all v, and hence $P_f\eta P_f\eta = 0$. ∎

Note that for $M \geq 1$ this construction only gives $((k, M, d))$ quantum error correcting codes for which the minimum distance d is at most $\lceil \frac{k+3}{2} \rceil$. This is because any $k+1$ columns of the matrix A_f are linearly dependent, which means that there is a $2k$ bit vector w of symplectic weight at most $\lceil \frac{k+1}{2} \rceil$ such that $[x_1, x_2, ...x_{2k}] * w^T = 0$, and the zero vector is never in $Cset_f$.

Lemma 8: A $((k, M, d))$ additive QECC exists when

1) $M = 2^m$ for some m
2) There are $2k$ binary k-tuples $x_1, x_2, ..., x_{2k}$ such that $Cset_f$ for $f(v) = v_k v_{k-1} ... v_{m+1}$ contains the set $\{[x_1, x_2, ...x_{2k}] * w^T |$ w is a 2k bit vector of symplectic weight $\leq d-1\}$. The rows of the matrix A_f = $[x_1 x_2 .....x_{2k}]_{k \times 2k}$ have pairwise symplectic product zero and are linearly independent.

Remark 1: The projection operator corresponding to the QECC is $\prod_{i=m+1}^{k} \frac{1}{2}(I + E_{y_i})$ where y_i is $k+1-i^{th}$ row of A_f. The quantum code obtained in this way is that formed in the stabilizer framework using $E_{y_k}, E_{y_{k-1}}, ..., E_{y_{m+1}}$ as the stabilizers of the code.

Proof: By Theorem 2 there exists a $((k, M, d))$-QECC. The construction method of Theorem 2 gives the corresponding projection operator as $P_f = \prod_{i=m+1}^{k} P_i = \prod_{i=m+1}^{k} \frac{1}{2}(I + E_{y_i})$. Any vector in the code subspace is given by $|x> = P_f|u>$ for some $|u> \in H$. Since E_{y_i} and E_{y_j} are commutative, we have $E_{y_i}|x> = |x>$ for $m < i \leq k$. Hence, $E_{y_k}, E_{y_{k-1}}, ..., E_{y_{m+1}}$ are the stabilizers of the quantum code and the quantum code is additive. ∎

Remark 2: If the boolean function can be represented as a single monomial, it gives an additive code. The converse is not true in general; see for example, [22], where it is shown that every $((4, 4, 2))$ code is equivalent to an additive code.

Example 5: For $m \geq 2$, we construct a $((2m, 4^{m-1}, 2))$ additive QECC as an example of the above approach. Note that Rains [22] has shown that $M \leq 4^{m-1}$ for any $((2m, M, 2))$ quantum code and this example meets the upper bound. Take $f(v) = v_{2m} v_{2m-1}$. It is a function of $k = 2m$ variables with Hamming weight 4^{m-1} and the corresponding complementary set is $\{(010..0), (010...01), ...(111...1)\}$ (or $\{4^{m-1}, 4^{m-1} + 1, ..., 4^m - 1\}$ in decimal notation). This complementary set contains the set $\{x_1, x_2, ..., x_{2k}, x_1 \oplus x_{k+1}, ..., x_k \oplus x_{2k}\}$ where x_1 = x_2 = ... = x_k = (0 1 0 .. 0) (or 4^{m-1}), x_{k+1} = (1 0 1 .. 1), x_{k+2} = (1 0 1 0 .. 0), x_{k+3} = (1 0 0 1 0 .. 0), .. , x_{2k-1} = (1 0 0 .. 0 1) and x_{2k} = (1 0 0 .. 0). The matrix A_f is given by

$$A_f = \begin{array}{c} \begin{matrix} x_1 & \dots & x_k & & & & \dots & & & x_{2k} \end{matrix} \\ \left(\begin{array}{cccc|ccccccc} 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & \dots & 0 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \dots & 0 & 1 & 0 \end{array} \right) \end{array}$$

We see that the symplectic inner product of any two rows is zero. Hence, we have constructed a $((2m, 4^{m-1}, 2))$ QECC. Tracing through the construction of the projection operator P_f we find that $P_f = P_{2m} P_{2m-1}$, where $P_i = \frac{1}{2}(I + E_{v_i})$ and v_i is the $(2m+1-i)^{th}$ row of the matrix A_f. Hence, $P_{2m} = \frac{1}{2}(I + E_{00..0|11..1})$ and $P_{2m-1} = \frac{1}{2}(I + E_{11..1|00..0})$.

Example 6: For $m \geq 3$, we construct a $((2m, 4^{m-1}, 2))$ QECC that is not additive as an example of the above approach. Consider the Boolean function $f(v) = v_{2m} v_{2m-1} v_{2m-2} + v_{2m} v_{2m-1} \bar{v}_{2m-2} (v_{2m-3} + \bar{v}_{2m-3} v_{2m-4} + \bar{v}_{2m-3} \bar{v}_{2m-4} v_{2m-5} + ... + \bar{v}_{2m-4} \bar{v}_{2m-3} ... \bar{v}_2 v_1) + v_{2m} \bar{v}_{2m-1} v_{2m-2} ... v_1$. It is a function of $k = 2m$ variables with weight 4^{m-1}, and the corresponding complementary set is $\{(011..1), (100...0), (100...1), ...(111...1)\}$ (or $\{2^{2m-1} - 1, 2^{2m-1}, ..., 4^m - 1\}$ in decimal notation). This complementary set contains the set $\{x_1, x_2, ..., x_{2k}, x_1 \oplus x_{k+1}, ..., x_k \oplus x_{2k}\}$ where x_1 = x_2 = ... = x_k = (0 1 1 .. 1) (or $2^{2m-1} - 1$), x_{k+1} = (1 0 1 .. 1), x_{k+2} = (1 0 1 0 .. 0), x_{k+3} = (1 0 0 1 0 .. 0),

.. , x_{2k-1} = (1 0 0 .. 0 1) and x_{2k} = (1 0 0 .. 0). The matrix A_f is given by

$$A_f = \begin{array}{c} \begin{matrix} x_1 & \dots & x_k & & & & \dots & & & x_{2k} \end{matrix} \\ \left(\begin{array}{ccc|ccc|ccc} 0 & \dots & 0 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & \dots & 1 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & \cdots & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & \cdots & 1 & 1 & 0 & 0 & \dots & 1 & 0 & 0 \\ 1 & \cdots & 1 & 1 & 0 & 0 & \dots & 0 & 1 & 0 \end{array} \right) \end{array}$$

We can also see that the second property is satisfied, so we have constructed a $((2m, 4^{m-1}, 2))$ QECC that is not additive.

Example 7: The $((5, 6, 2))$-QECC constructed by Rains *et al.* [21] is also a special case of the above procedure. Take the Boolean function $f(v) = v_1v_2v_3 \oplus v_3v_4v_5 \oplus v_2v_3v_4 \oplus v_1v_2v_5 \oplus v_1v_4v_5 \oplus v_2v_3v_4v_5$. It is a function of 5 variables with weight 6, and the corresponding complementary set is $\{1, 3, 4, 6, 8, 11, 12, 14, 17, 19, 21, 22, 24, 26, 28, 31\}$. Take ($x_1$, ... , x_{10}) to be (6, 12, 24, 17, 3, 14, 31, 28, 26, 22) and form the matrix

$$A_f = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

The symplectic inner product of any two rows is zero and the corresponding projection operator P_f coincides with the one determined by the $((5, 6, 2))$-QECC in [21].

Lemma 9: 1) If there exists a $((k, M, 2))$ QECC, then there exists a $((k + 2, 4M, 2))$ QECC determined by $f'(v_1, v_2, ..., v_{k+2}) = f(v_1, v_2, ..., v_k)$ and $A_{f'} = (x_1, x_2, \dots, x_{k-1}, x_k, x_k, x_k, x_{k+1}, x_{k+2}, \dots, x_{2k-1}, 2^{k+1} + 2^k + x_{2k}, 2^k + x_{2k}, 2^{k+1} + x_{2k})$

2) If there exists a $((k, M, 2))$ QECC, then there exists a $((k, M-1, 2))$ QECC determined by same A_f and $f'(v)$ having support a subset of $f(v)$.

Proof:

1) Let $f(v_1, v_2, .., v_k)$ be the weight M Boolean function corresponding to the $((k, M, 2))$-QECC. The Boolean function $f'(v_1, v_2, ..., v_{k+2}) = f(v_1, v_2, ..., v_k)$ has weight $4M$, and the complementary set $Cset_{f'}$ has vectors of length $k + 2$ which are of the form $\{(\{0, 1\}, \{0, 1\}, x) : x \in Cset_f\}$. This means that $Cset_{f'}$ has 4 times as many elements as $Cset_f$. Note that if $x_1, x_2, ..., x_{2k}, x_1 \oplus x_{k+1}, ..., x_k \oplus x_{2k}$ are in $Cset_f$, then $(0, 0, x_1), (0, 0, x_2)$, $...(0, 0, x_{2k-1})$, $(1, 1, x_{2k})$, $(0, 1, x_{2k})$, $(1, 0, x_{2k})$, $(0, 0, x_1 \oplus x_{k+1})$, ..., $(0, 0, x_{k-1} \oplus x_{2k-1})$, $(1, 1, x_k \oplus x_{2k})$, $(0, 1, x_k \oplus x_{2k})$, $(1, 0, x_k \oplus x_{2k})$ are in $Cset_{f'}$. Let $A_{f'} = ((0, 0, x_1), (0, 0, x_2), \dots , (0, 0, x_{k-1}), (0, 0, x_k), (0, 0, x_k), (0, 0, x_k), (0, 0, x_{k+1}), (0, 0, x_{k+2}), \dots , (0, 0, x_{2k-1}), (1, 1, x_{2k}), (0, 1, x_{2k}), (1, 0, x_{2k}))$. All the columns and the sum of columns i and $i + k$ are in $Cset_{f'}$. The symplectic product of any two rows is zero and all the rows are linearly independent, since this was true for $A_f = (x_1, x_2, \dots, x_{2k})$

2) Given this choice of $f'(v)$, we have $Cset_{f'} \supseteq Cset_f$, and this means that the same matrix $A_{f'} = A_f$ will satisfy all the earlier properties.

■

Example 8: We will now use Lemma 9 to extend the Rains code to a $((2m + 1, 3 \times 2^{2m-3}, 2))$-QECC for $m > 2$.

Consider the Boolean function f(v) = $v_1v_2v_3 \oplus v_3v_4v_5 \oplus v_2v_3v_4 \oplus v_1v_2v_5 \oplus v_1v_4v_5 \oplus v_2v_3v_4v_5$. It is a function of $2m+1$ variables with weight $3 \times 2^{2m-3}$.

Let (x_1, ... x_{2m+1}) be (6, 12, 24, 17, 3,3,...3) and (x_{2m+2}, ... x_{4m+2}) be (14, 31, 28, 26, $2^{2m+1} - 10$,$2^5 + 22$, $2^6 + 22$, ... $2^{2m} + 22$). The matrix A_f is then

$$\left(\begin{array}{ccccccc|ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & \dots & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 & 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 & 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & \dots & 1 & 1 & 1 & 0 & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & \dots & 1 & 0 & 1 & 0 & 0 & 0 & 0 & \dots & 0 \end{array} \right)$$

We see that symplectic product of any two rows is zero. Hence, we have constructed a $((2m + 1, 3 \times 2^{2m-3}, 2))$ non-additive QECC.

Example 9: The perfect $((5, 2, 3))$ additive code of R. Laflamme *et al.* [17] can be obtained by the above approach. Take $f(v) = v_5v_4v_3v_2$. The corresponding complementary set is $\{2, 3, ...31\}$. The matrix A_f is given by

$$A_f = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

it is easy to see that all rows are linearly independent, and that the symplectic inner product of any two rows is zero. Note that the stabilizers corresponding to the code are $ZXXZI$, $IZXXZ$, $ZIZXX$, and $XZIZX$.

VII. Operator Quantum Error Correction (OQEC)

The theory of operator quantum error correction [16] uses the framework of noiseless subsystems to improve the performance of decoding algorithms which might help improve the threshold for fault-tolerant quantum computation. It requires a fixed partition of the systems Hilbert space $H = A \otimes B \oplus C^{\perp}$. Information is encoded on the A subsystem; the logical quantum state $\rho_A \in \mathbb{B}_A$ is encoded as $\rho_A \otimes \rho_B \oplus 0^{C^{\perp}}$ with an arbitrary $\rho_B \in \mathbb{B}_B$ (where $\mathbb{B}_A$ and $\mathbb{B}_B$ are the sets of all endomorphisms on subsystems A and B respectively). We say that the error E is correctable on subsystem A (called

the logical subsystem) when there exists a physical map R that reverses its action, up to a transformation on the B subsystem (called the Gauge subsystem). In other words, this error correcting procedure may induce some nontrivial action on the B subsystem in the process of restoring information encoded in the A subsystem. This leads to recovery routines which explicitly make use of the subsystem structure [6][24]. In the case of standard quantum error correcting codes, the dimension of B is 1. A $((k, M, N, d))$-OQEC is defined as a OQEC in $\mathbb{C}^{2^k}$ with M and N as the dimension of the logical and gauge subsystems.

Lemma 10: A Boolean function f with the following properties determines $((k, 2^t, 2^{s-t}, d))$ stabilizer OQEC

1) $f(v)$ is of the form $v_k v_{k-1}..v_{s+1}$ with weight 2^s
2) There are $2k$ binary k-tuples $x_1, x_2, ..., x_{2k}$ such that $Cset_f$ contains the set $\{[x_1, x_2, ...x_{2k}] * w^T |\ w$ is a 2k bit vector of symplectic weight $\leq d-1\}$. The rows of the matrix $A_f = [x_1 x_2 .....x_{2k}]_{k\times 2k}$ have pairwise symplectic product zero and are linearly independent.

Proof: By Lemma 8, $f(v)$ satisfies the conditions for construction of an additive $((k, 2^s, d))$-QECC. The first $k-s$ rows of the matrix A_f are the stabilizers of the code, and using this QECC, we construct an OQEC following [19].

We denote by X_j the matrix X (the Pauli matrix) acting on the j^{th} qubit, and similarly for Y_j and Z_j. The Heisenberg-Weyl group $E_k =< i, X_1, Z_1, ..., X_k, Z_k >$. The first step in constructing a stabilizer code is to choose a set of $2k$ operators $\{X'_j, Z'_j\}_{j=1,..,k}$ from E_k that is Clifford isomorphic to the set of single-qubit Pauli operators $\{X_j, Z_j\}_{j=1,..,k}$ in the sense that the primed and unprimed operators obey the same commutation relations. The operators $\{X'_j, Z'_j\}_{j=1,..,k}$ generate P_k and behave as single-qubit Pauli operators. We can think of them as acting on k virtual qubits.

Form Z'_1, ... , Z'_k corresponding to the rows of matrix A_f. (The image of the first row in the Heisenberg-Weyl group gives Z'_1 and so on.) Given all the Z'_j, we can easily find X'_j which have symplectic product of 1 with X'_j and symplectic product of 0 with all other X'_l, $l \neq j$.

Hence, the stabilizer group is given by $S =< Z'_1, Z'_2, ..., Z'_{k-s} >$. If we want to construct a $((k, 2^t, 2^{s-t}, d))$-OQEC, then we need to find a subsystem of dimension 2^t in the above subspace C of dimension 2^s. Following [19], if we take the Gauge group (corresponding to the Gauge subsystem defined before) $G =< S, X'_{k-s+1}, Z'_{k-s+1}, ..., X'_{k-t}, Z'_{k-t} >$ and the logical group $L =< X'_{k-t+1}, Z'_{k-t+1}, ..., X'_k, Z'_k >$, the action of any $l \in L$ and $g \in G$ restricted to the code subspace C is given by

$$gP = I_A \otimes g^B$$
$$lP = l^A \otimes I_B$$

for some l^A, g^B in $\mathbb{B}_A$ and $\mathbb{B}_B$ respectively, where A and B are the required subsystems. Since we are encoding in a subsystem of the subspace formed by $((k, 2^s, d))$-QECC, the minimum distance of the OQEC thus obtained will be $\geq d$. ■

VIII. Conclusion

We have described a fundamental correspondence between Boolean functions and projection operators in Hilbert space that provides a mathematical framework that unifies the construction of additive and non-additive quantum codes. We have given sufficient conditions for the existence of QECC in terms of existence of a Boolean function satisfying certain properties and presented examples of Boolean functions satisfying these properties. We have also given a method to construct the quantum code if these properties are satisfied. Our method leads to a construction of $((2m, 4^{m-1}, 2))$ codes, the original $((5, 6, 2))$ code constructed by Rains *et al.*, the extension of this code to $((2m+1, 3\times 2^{2m-3}, 2))$ codes, and the perfect $((5, 2, 3))$ code. Finally we have shown how the new framework can be integrated with operator quantum error correcting codes.

IX. Acknowledgements

The authors would like to thank the anonymous reviewers for many suggestions that improved this paper and for bringing the work of Danielson [11] to their attention.

References

[1] V. Aggarwal, A. Ashikhmin and A.R. Calderbank, "A Grassmannian packing based on the Nordstrom-Robinson code," *Proc. IEEE Information Theory Workshop*, pp. 1-5, Chengdu, China, Oct. 2006.

[2] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, "Remarkable degenerate quantum stabilizer codes derived from duadic codes," *quant-ph/0601117*, Jan. 2006.

[3] A. Ashikhmin and A.R. Calderbank, "Space-time Reed-Muller codes for noncoherent MIMO transmission," *IEEE International Symposium on Information Theory*, pp. 1952-1956, Adelaide, Australia, Sept. 2005.

[4] A. Ashikhmin and S. Litsyn, "Foundations of quantum error correction," *Recent Trends in Coding Theory and its Applications*, 2007.

[5] V. Arvind, P.P. Kurur and K.R. Parthasarathy, "Nonstabilizer quantum codes from abelian subgroups of the error group," *quant-ph/0210097*.

[6] D. Bacon, "Operator quantum error-correcting subsystems for self-correcting quantum memories," *Phys. Rev. A 73*, 012340, 2006.

[7] A.R. Calderbank, E.M. Rains, P.M. Shor and N.J.A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, Jul 1998.

[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry", *Phys. Rev. Lett*, vol. 78, pp. 405-409, 1997.

[9] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A* 54, pp. 1098-1105, 1996.

[10] D.W. Cohen, "An introduction to Hilbert space and quantum logic," *Springer-Verlag*, 1989.

[11] L.E. Danielson, "On self-dual quantum codes, graphs, and Boolean functions," *quant-ph/0503236*, Master's thesis, University of Bergen, Norway, Mar. 2005.

[12] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett. 77*, pp. 2585-2588, Sept. 1996.

[13] M. Grassl and T. Beth, "A note on non-additive quantum codes," *quant-ph/9703016*, March 1997.

[14] D. Gottesman, "Stabilizer codes and quantum error correction," *PhD Thesis*, quant-ph/9705052.

[15] A. Ketkar, A. Klappenecker, S. Kumar and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Transactions on Information Theory*, pp. 4892-4914, Nov. 2006.

[16] D. Kribs, R. Laflamme and D. Poulin, "Unified and generalized approach to quantum error correction," *Phys. Rev. Lett. 94*, 180501, 2005.

[17] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett. 77*, pp. 198-201, 1996.

[18] S. Lipschutz, "Schaum's Outline of Theory and Problems of Essential Computer Mathematics," *McGraw-Hill*, 1982.

[19] D. Poulin, "Stabilizer formalism for operator quantum error correction," *quant-ph/0508131*, Jun 2006.

[20] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, “Propagation characteristics of Boolean functions,” *Lecture Notes in Computer Science, Springer- Verlag*, pp. 161-173 (1991).
[21] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, “A nonadditive quantum code,” *Phys. Rev. Lett. 79*, pp. 953-954, 1997.
[22] E.M. Rains, “Quantum codes of minimum distance two,” *IEEE Transactions on Information Theory*, pp. 266-271, Jan 1999.
[23] V. P. Roychowdhury and F. Vatan, “On the existence of nonadditive quantum codes”, *Lecture notes in computer science*, Springer, 1998.
[24] P. Zanardi, D. A. Lidar, and S. Lloyd, “Quantum tensor product structures are observable induced,” *Phys. Rev. Lett. 92*, 060402, 2004.